Federal Computer Incident Response Center

The FedCIRC Bits & Bytes

A monthly newsletter for Information System Security Managers/Officers & System Administrators

May 1, 2001 Volume II, Issue 4

A Note from the Director

We are glad to announce the addition of a new partner to our Federal incident response community. Global Integrity has joined us in our collective effort to assist in securing our information systems and responding to incidents. Global Integrity brings a wealth of knowledge, and experience, with an expanded view by maintaining two operating centers outside the United States. One in Japan, and the other in Europe. This global perspective will provide the added advantage needed in defending against costly intrusions. As the operational arm of FedCIRC, Global Integrity will maintain and operate a 24/7/365 FedCIRC Security Operations Center (F-SOC) in Northern Virginia. F-SOC will assume those day-to-day incident-handling functions previously performed by Carnegie Mellon's CERT Coordination Center (CERT-CC). CERT-CC will refocus all of their efforts on incident and vulnerability analysis. It goes without saying that the CERT-CC has and will continue to support FedCIRC with their traditional superior efforts and results. They have always been up to the challenge regardless of the prevailing threat.

The FedCIRC hotline number, 888-282-0870 will not change. Effective April 27, 2001 the new number for facsimile service will be 703-375-2427. Please make note of the change and update your FedCIRC contact records.

Thanks to the entire CERT-CC staff, past and present and warm welcome aboard to those at Global Integrity.

Note: Global Integrity is a partner of Science Applications International (SAIC)

Warning Notices

Are you being bombarded by computer security warnings on viruses, trojans, worms, denial of service attacks, and system vulnerabilities? Certainly, we've come from famine to an abundance of warning products. Although the shear number of warning notices received may be irritating at times, on this particular issue, more *is* better.

However, we should exercise concerns regarding those elements that affect the validity and value of such products, and how seriously we take them. Organizations that issue warnings take a number of risks. They effectively walk the proverbial "tight rope". If the warning turns out to be a false alarm, the organization's credibility is questioned. On the other hand, the organization that waits a little too long to issue a warning may be criticized for not sharing information quick enough. Also, a warning product fraught with errors, or having little relevance may not be taken seriously the next time. Let's hope we continue to take each warning notice in a serious manner regardless of its applicability and when necessary, take immediate action.

The sources of warning products are many and include FedCIRC, NIPC, JTF-CNO, CERT-CC, anti-virus vendors, and a host of other information security-centric organizations. We all strive to issue credible, accurate and timely products with respect to our individual missions. FedCIRC is the central coordinating organization for dealing with computer security related incidents affecting Federal civilian agencies and departments of the government. It facilitates communication and information sharing among its constituents and collaborates with elements of government, industry, academia and law enforcement.

continued on Page 2....

continued from Page 1...

Regardless of the source, FedCIRC may be contacted if you have questions concerning a warning product.

The NIPC has a broad mission that encompasses components of the nation's critical infrastructures. The balancing act of sharing information and conducting an investigation is challenging and makes the task of preparing a warning product a difficult process. The NIPC manages to do a good job under demanding circumstances and continues to forge onward in accomplishing its mission.

As the response activity for the Department of Defense and military services, the JTF-CNO is well prepared in maintaining vigilance over the many diverse DoD systems. Although it may be a rarity for a civil agency to receive a warning product directly from the JTF-CNO, it occasionally does happen. Receipt of any such information should always be authenticated before redistributing or taking any associated action.

Since 1989, the Carnegie Mellon University, Software Engineering Institute’s CERT-CC has been a major player in incident response, and advising the information security professionals on system vulnerabilities. The CERT-CC has been the quintessential entity serving the community at the highest level. They are frequently relied on to validate and coordinate warning products. Certainly not to be forgotten are our private industry partners. They are frequently in the forefront in identifying and reporting system vulnerabilities. They are on the front lines and time and again respond to the initial outburst of attacks by intruders.

It’s easy to see how the volumes of warning information received can overwhelm us. However, as stated earlier, more is better. Each responsible reporting organization improves their product over time. A key step in our continued improvement is the constructive feedback received from the recipients of our respective products. Keep your comments coming.

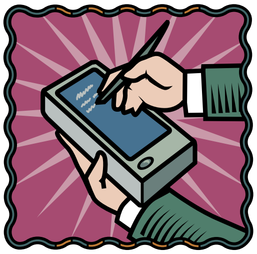
FY- 01 Statistics

FY- 01, FedCIRC has responded to 374 incidents affecting 36,562 hosts.

FedCIRC has also issued:
- 12 Security Alerts
- 3 Incident Notes
- 0 Vulnerability Notes

Partner Support

In support of our national effort to protect our critical infrastructures, FedCIRC fully supports the objectives of PDD-63. In addition to those agencies with infrastructure liaison responsibilities, FedCIRC continues to provide staff support to the National Infrastructure Protection Center (NIPC). On April 16, 2001, Mr. Kenneth Grossman began a one-year detail to the NIPC's Analysis and Warning Section, Watch and Warning Unit (WWU). Ken brings a wealth of knowledge and experience and will provide a different perspective to the NIPC. Prior to Ken's assignment, Michael C. Smith completed a 20-month detail as the Deputy Unit Chief of the NIPC's WWU. Michael returned to FedCIRC on March 5, 2001, and will be managing some of the ongoing FedCIRC initiatives.



Security Related Websites

Security websites:

http://www.boran.com/security

http://www.nsi.org/compsec.html

http://www.atstake.com

http://xforce.iss.net

http://www.securityportal.com

Calendar of Events

Fundamentals of Information Security
Dates: May 7-9, July 9-11, or Oct 15-17, 2001
Locations: varies
POC: MIS Training Institute
508-879-7999
http://www.misti.com/seminar_list.asp

Developing and Writing Information Security Policies
Dates: June 14-15, July 12-13, Oct 1-2, or Dec 3-4, 2001
Locations: varies
POC: MIS Training Institute
508-879-7999
http://www.misti.com/seminar_list.asp

NETSEC'01
Date: June 18-20, 2001
Location: New Orleans, LA
POC: Computer Security Institute
415-947-6320,
http://www.gocsi.com/#netsec_01

Concepts and Trends in Information Security
Date: July 17, 2001
Location: Arlington, VA
POC: Carnegie Mellon Univ, Software Engineering Institute (CERT-CC)
412-268-7702
http://www.cert.org/nav/training.html

Computer Security Incident Handling for Technical Staff (Advanced)
Date: August 6-10, 2001
Location: Pittsburgh, PA
POC: Carnegie Mellon Univ, Software Engineering Institute (CERT-CC)
412-268-7702
http://www.cert.org/nav/training.html

Latest FedCIRC Advisories

FedCIRC Advisory FA-2001-05
Exploitation of snmpXdmid

FedCIRC Advisory FA-2001-06
Automatic Execution of Embedded MIME Types

FedCIRC Advisory FA-2001-07
File Gobbling Vulnerabilities in Various FTP Servers

FedCIRC Advisory FA-2001-08
Multiple Vulnerabilities in Alcatel ADSL Modems

The FedCIRC Bits & Bytes Newsletter

Director
David Jarrell
Project Manager for Marketing/Outreach
Connie Oden
Editor
Corliss McCain
Contributing Editors
David Adler
Kenneth Grossman
Corliss McCain
Michael Smith

We welcome your input! To submit your related articles and notices for future issues, please contact FedCIRC at 202-708-5060. Deadline for submissions is the 15th of each month. Articles may be edited for length and content. Back issues of this newsletter can be found on the FedCIRC website www.fedcirc.gov/docs.html

FedCIRC is sponsored by the Federal CIO Council and is operated by the General Services Administration/Federal Technology Service